Compensating Controls for Advanced Authentication for Smartphones or Tablets

The APB has passed a Compensating Controls for Advanced Authentication policy for use with Agency issued and controlled Smartphone or Tablets. The compensating controls may be used under these very specific conditions in lieu of Advanced Authentication for these types of devices in the State of Texas.

The Texas CSO has put in place the following process for approval of the compensating controls in the policy:

- The Smartphone or Tablet must be Agency owned.
- Mobile Device Management software must be implemented to control these devices.
- A minimum of four of the listed examples in the policy must be implemented.
- An email must be sent to securitycommittee@dps.texas.gov requesting conditional approval of the compensating controls.
    - The "Subject line" should read – Request for AA Compensating Control Approval.
    - The body should include your Agency name and contact information and a list of implemented controls from the policy.
- The email should be kept and will be a required item at the agency's next on-site technical audit.

If the above process is completed, it will result in conditional approval of your compensating controls for Advanced Authentication until the Technical Audit team can arrive on-site to perform an audit of the agency's implementation. After approval, you may proceed with a Smartphone or tablet implementation at the agency.

How does this change impact Texas Agencies?

For agencies that want to deploy Smartphones or tablets, but are unable to meet current Advanced Authentication methods, the agency can submit properly configured Compensating Control methods for conditional approval.

This change to the policy should be reflected in CSP version 5.3 that is expected in mid-2014. APB recommendations do not become official policy until they are signed by the Director of the FBI. This signature process can be lengthy. The purpose of this information is to make the agency aware of the recommended pending change.

Compensating Controls for Advanced Authentication (AA) Compliance When Using Agency Issued and Controlled Smartphones (and Tablets)

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel and technical security controls associated with the user location. For example, AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10). Conversely, if the technical security controls have not been met AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions.

CSO approved compensating controls to meet the AA requirement on agency issued smartphones are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. The compensating controls shall:

1. ***Meet the intent of the CJIS Security Policy AA requirement***
2. ***Provide a similar level of protection or security as the original AA requirement***
3. ***Not rely upon the existing requirements for AA as compensating controls***

Mobile Device Management (MDM) must be implemented and provide at least two of the other examples of compensating controls listed below.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The proposed compensating controls for AA are a combination of controls that provide acceptable assurance it's the authorized user authenticating and not an impersonator or (in the case of agency issued devices used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

Examples of AA compensating controls(s) for and agency issued smartphones and tablets are:

- Possession of the agency issued smartphone as an indication it's the authorized user
- Implement password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assist decision makers in determining whether or not AA is required.

1. – 5. …

6. ***Is the user device an agency issued and controlled smartphone or tablet?***

   If both (a) and (b) below are true, the answer to the above question is "yes". Proceed to question 9.

   a. ***The law enforcement agency issued the device to an individual; and***
   b. ***The device is subject to administrative management control of the issuing agency.***

   If either (a) or (b) above are false then the answer is "no". Decision tree completed. AA required.

7. ***Does the agency issued smartphone have CSO-approved AA compensating controls implemented?***

   If (a) and (b) below, are true the answer to the above question is "yes". Decision tree completed. AA requirement is waived.

   a. ***An agency cannot meet a requirement due to legitimate technical or business constraints; and***
   b. ***The CSO has given written approval permitting AA compensating controls to be implemented in lieu of the required AA control measures***

   If either (a) or (b) above are false then the answer is "no". Decision tree completed. AA required.

Update Figure 10 to include #8 and #9 regarding compensating control as shown below:

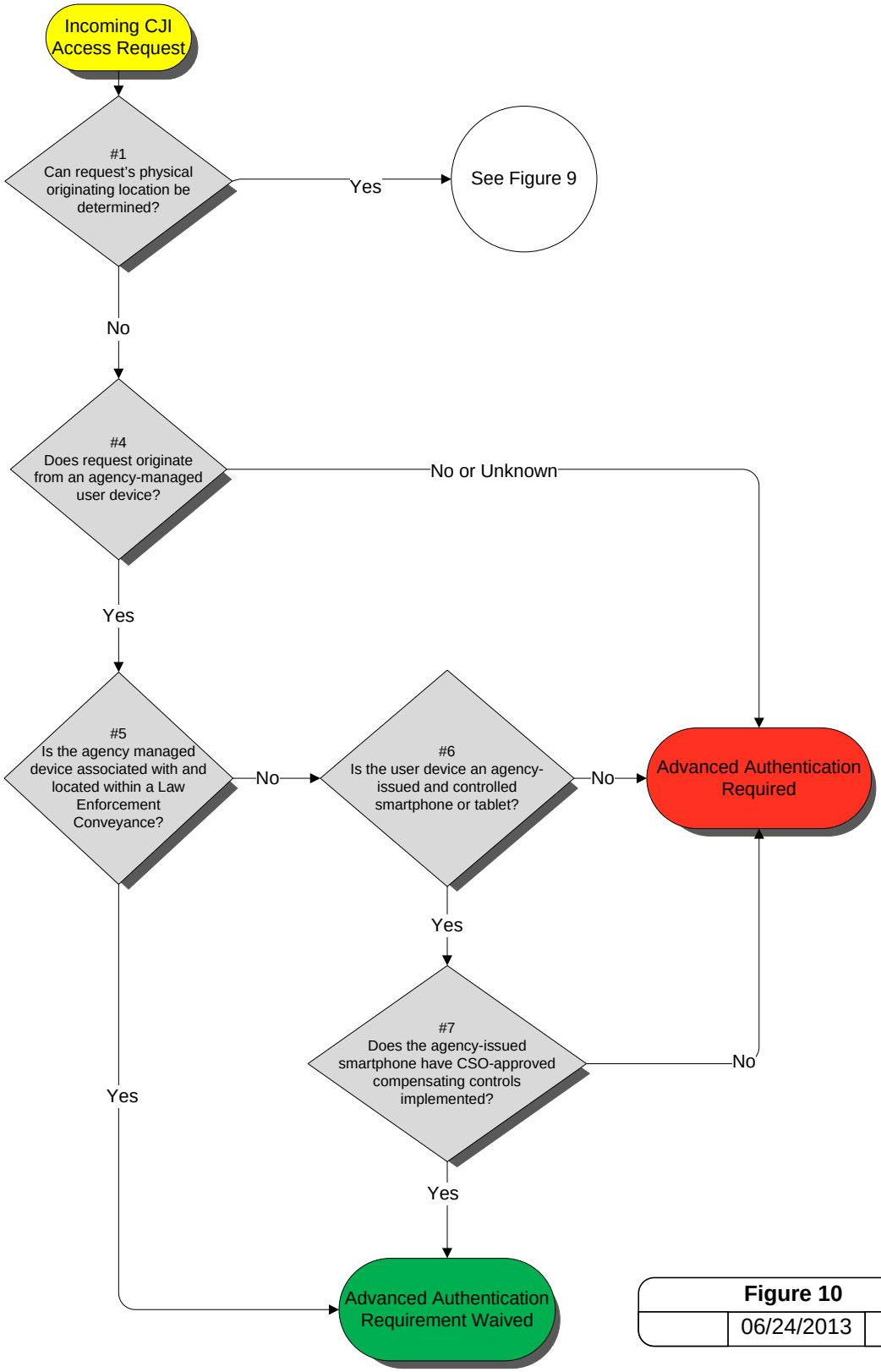

Figure 10
06/24/2013

Attachment # 2

Proposed definitions Proposed CJIS Security Policy Section Language Changes

Add Following Definitions to Appendix A:

Compensating Controls – Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Laptop Devices – Laptop devices are mobile devices with a full featured operating system (e.g. Microsoft Windows, Apple OS X, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited feature operating system (e.g. tablets).

Tablet Devices – Tablet devices are mobile devices with a limited feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full featured operating systems (e.g. laptops).

Pocket/Handheld Mobile Devices – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, Blackberry, etc.). This definition does not include tablet and laptop devices.

Smartphone – See pocket/handheld mobile devices.

Attachment # 3

Add Following Use Cases to Figure 8 – Advanced Authentication Use Cases:

Figure 8 – Advanced Authentication Use Cases

Use Case 7 – Advanced Authentication Compensating Controls on Agency Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user's job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meets the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device

2. Move the email client used to authenticate with the local agency inside an encrypted, password protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency issued smartphone.